CLAIMS

1. A method for maintaining privacy for transactions performable by a user device (20) having a security module (22) with a privacy certification authority computer (30) and a verification computer (40), the verification computer (40) having obtained public keys from the privacy certification authority computer (30) and from an issuer (10) that provides attestation of the security module (22), the method comprising the steps of:

- receiving a first and second set of attestation-signature values (DAA1, DAA2), the first set of attestation-signature values (DAA1) being generated by the user device (20) using first attestation values (AV1) obtained from the issuer (10) and the second set of attestation-signature values (DAA2) being generated by the user device (20) using second attestation values (AV2) obtained from the privacy certification authority computer (30);

- checking the validity of the first set of attestation-signature values (DAA1) with the public key of the issuer (10);

- checking the validity of the second set of attestation-signature values (DAA2) with the public key of the privacy certification authority computer (30); and

- verifying whether or not the two sets of attestation-signature values (DAA1, DAA2) relate to the user device (20).

2. The method according to claim 1, wherein the step of verifying comprises the step of: verifying that a first value is derived from a base value, comprised in the first set of attestation-signature values (DAA1), and identical to a second value that is derived from said base value and is comprised in the second set of attestation-signature values (DAA2).

3. The method according to claim 1, wherein the step of verifying comprises the step of: verifying a proof that the two attestation-signature values (DAA1, DAA2) are based on the first and second attestation values (AV1, AV2) that are derived from at least one common value (t).

4. The method according to claim 2, wherein the base value is different each time the method is applied.

5. The method according to claim 3, wherein the common value (t) is derived from an endorsement key (EK) that is related to the security module (22).

6. A method for maintaining privacy for transactions performable by a user device (20) having a security module (22) with a privacy certification authority computer (30) and a verification computer (40), the privacy certification authority computer (30) having obtained a public key from an issuer (10) that provides attestation of the security module (22); the method comprising the steps of:

- receiving an initial set of attestation-signature values (DAA1') from the user device (20), the initial set of attestation-signature values (DAA1') being generated by the user device (20) using first attestation values (AV1) obtained from the issuer (10);

- checking the validity of the initial set of attestation-signature values (DAA1) with the public key of the issuer (10);

- responsive to the checking step issuing second attestation values (AV2) that relate to the initial set of attestation-signature values (DAA1'); and

- providing the second attestation values (AV2) to the user device (20), a second set of attestation-signature values (DAA2) being derivable from the second attestation values (AV2),

wherein it is verifiable that a first set of attestation-signature values (DAA1) and the second set of attestation-signature values (DAA2) relate to the user device (20), the first set of attestation-signature values (DAA1) is generatable by the user device (20) using first attestation values (AV1) obtained from the issuer (10).

7. The method according to claim 6, wherein the step of issuing the second attestation values (AV2) further comprises the step of: receiving a request value from the user device (20) and verifying whether the request value relates to the initial set of attestation-signature values (DAA1').

8. A method for maintaining privacy for transactions performable by a user device (20) having a security module (22) with a privacy certification authority computer (30) and an verification computer (40), the user device (20) having obtained first attestation values (AV1)

from an issuer (10) and second attestation values (AV2) from the privacy certification authority computer (30), the method comprising the steps of:

- generating a first set of attestation-signature values (DAA1) by using the first attestation values (AV1) and a second set of attestation-signature values (DAA2) by using the second attestation values (AV2); and

- sending the first and second set of attestation-signature values (DAA1, DAA2) to the verification computer (40),

wherein the verification computer (40) is able to check the validity of the first set of attestation-signature values (DAA1) with an issuer public key (PK_I) of the issuer (10), the validity of the second set of attestation-signature values (DAA2) with an authority public key (PK_{PCA}) of the privacy certification authority computer (30), and

to verify that the two sets of attestation-signature values (DAA1, DAA2) relate to the user device (20).

9. The method according to claim 8, wherein the step of generating comprises using an endorsement key (EK) that is related to the security module (22).

10. A computer program element comprising program code means for performing the method of any one of the claims 1 to 9 when said program is run on a computer.

11. A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform the method according to any one of the claims 1 to 9.

12. A system for maintaining privacy while computers performing transactions comprising:

an issuer (10) providing an issuer public key (PK_I);

a user device (20) having a security module (22) for generating a first set of attestation-signature values (DAA1);

a privacy certification authority computer (30) for providing an authority public key (PK_{PCA}) and issuing second attestation values (AV2); and

a verification computer (40) for checking the validity of the first set of attestation-signature values (DAA1) with the issuer public key (PK_I) and the validity of a second set of attestation-signature values (DAA2) with the authority public key (PK_{PCA}), the second set of attestation-signature values (DAA2) being derivable by the user device (20) from the second attestation values (AV2),

wherein it is verifiable that the two sets of attestation-signature values (DAA1, DAA2) relate to the user device (20).

* * *